09/763104

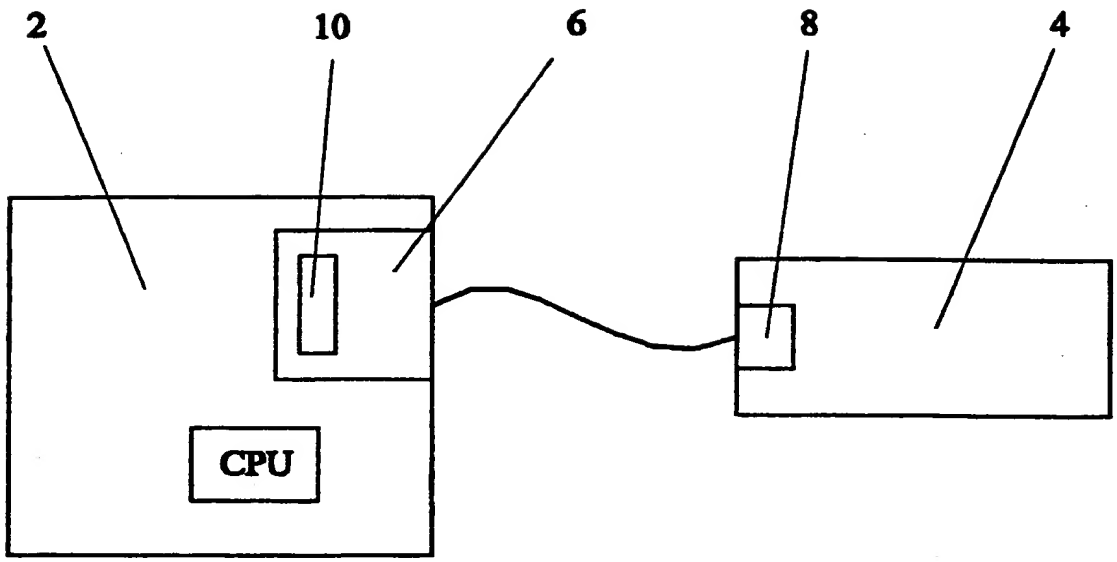


FIG. 1

BOCID: WO 0011536A1

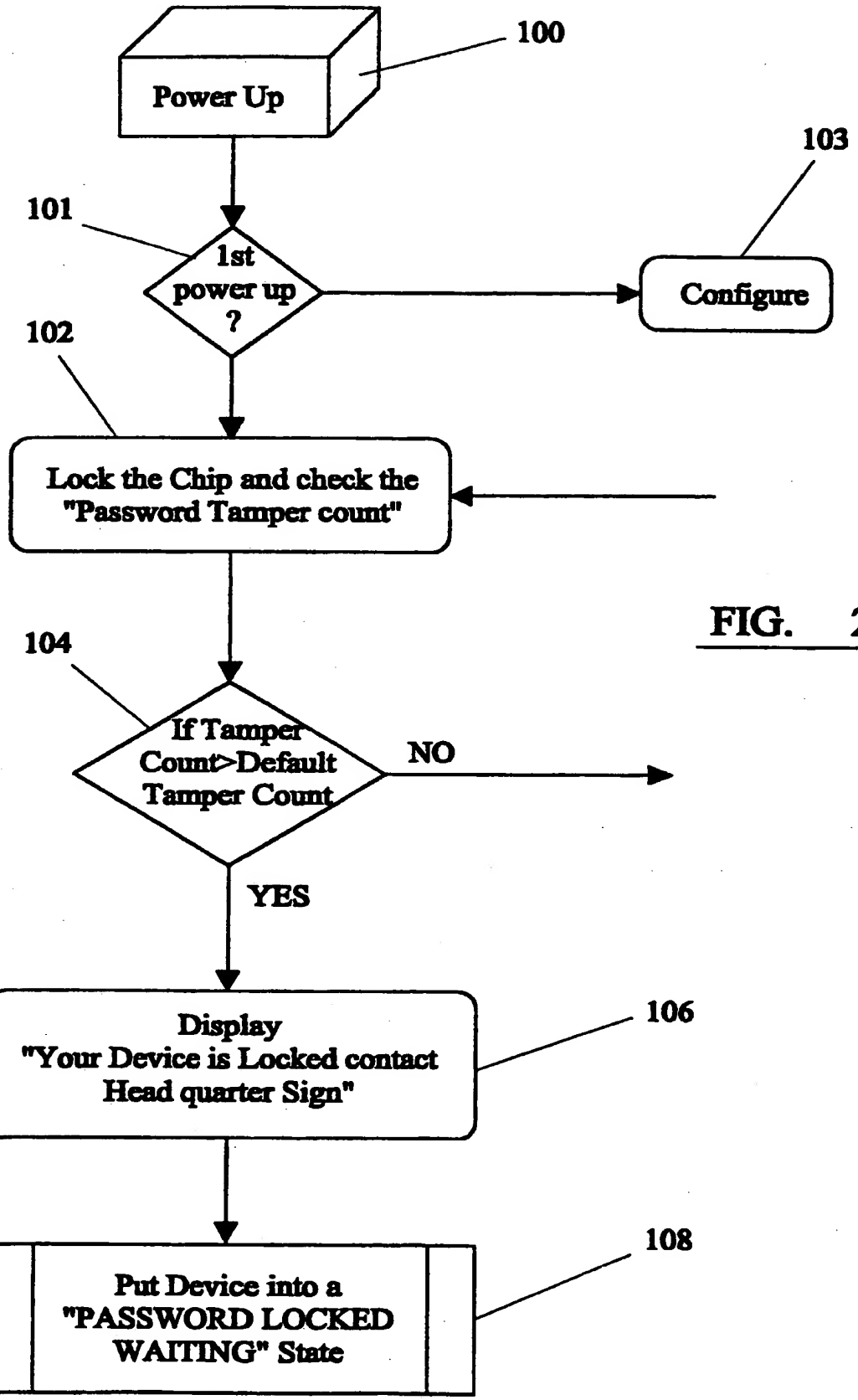

100
Power Up
103
101
1st power up ?
Configure
102
Lock the Chip and check the "Password Tamper count"
104
If Tamper Count>Default Tamper Count
NO
YES
Display "Your Device is Locked contact Head quarter Sign"
106
Put Device into a "PASSWORD LOCKED WAITING" State
108

FIG. 2A

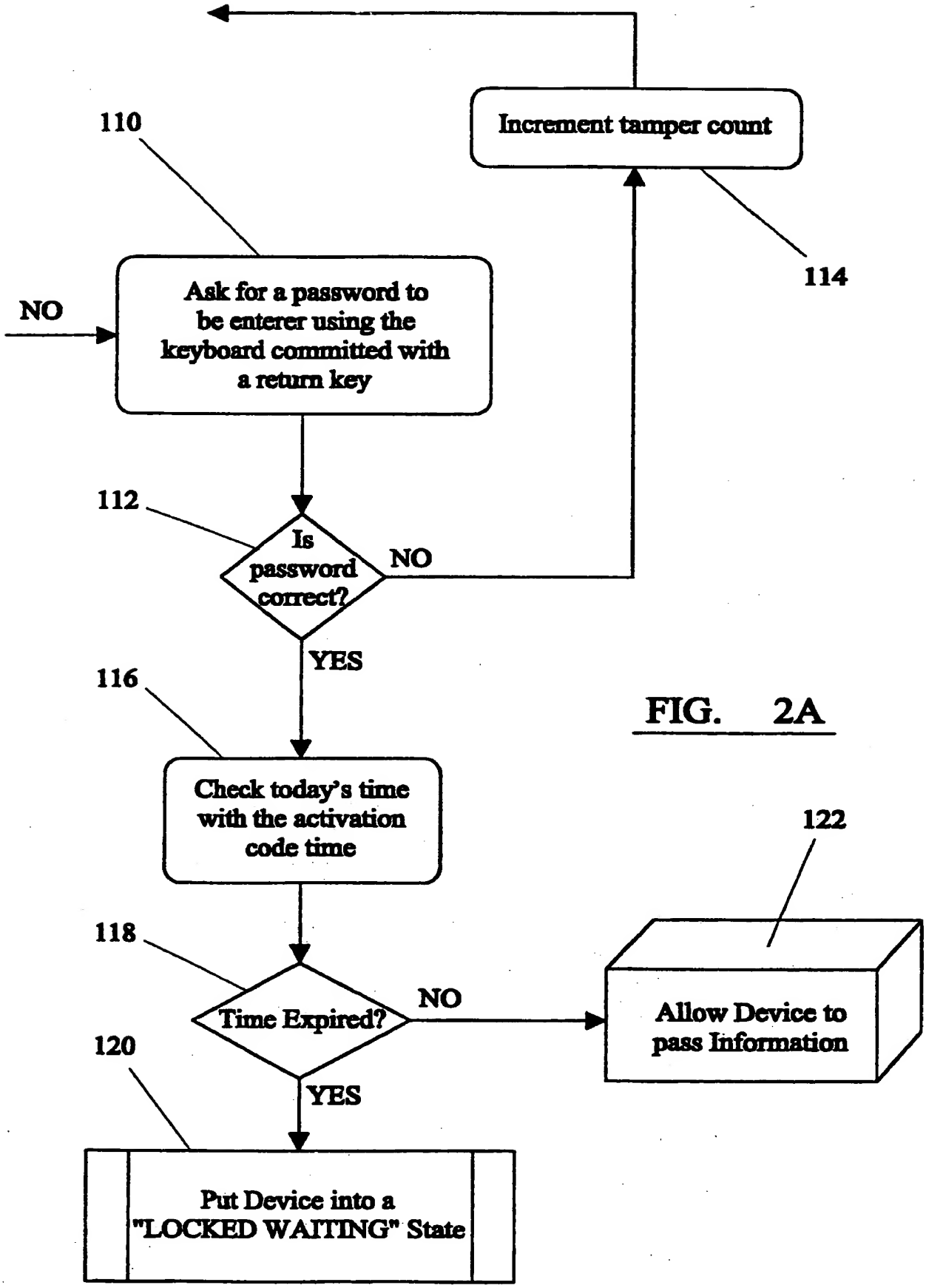

110
Ask for a password to be enterer using the keyboard committed with a return key
NO
112
Is password correct?
NO
YES
114
Increment tamper count
116
Check today's time with the activation code time
118
Time Expired?
NO
YES
120
Put Device into a "LOCKED WAITING" State
122
Allow Device to pass Information

FIG. 2A

FIG. 2B

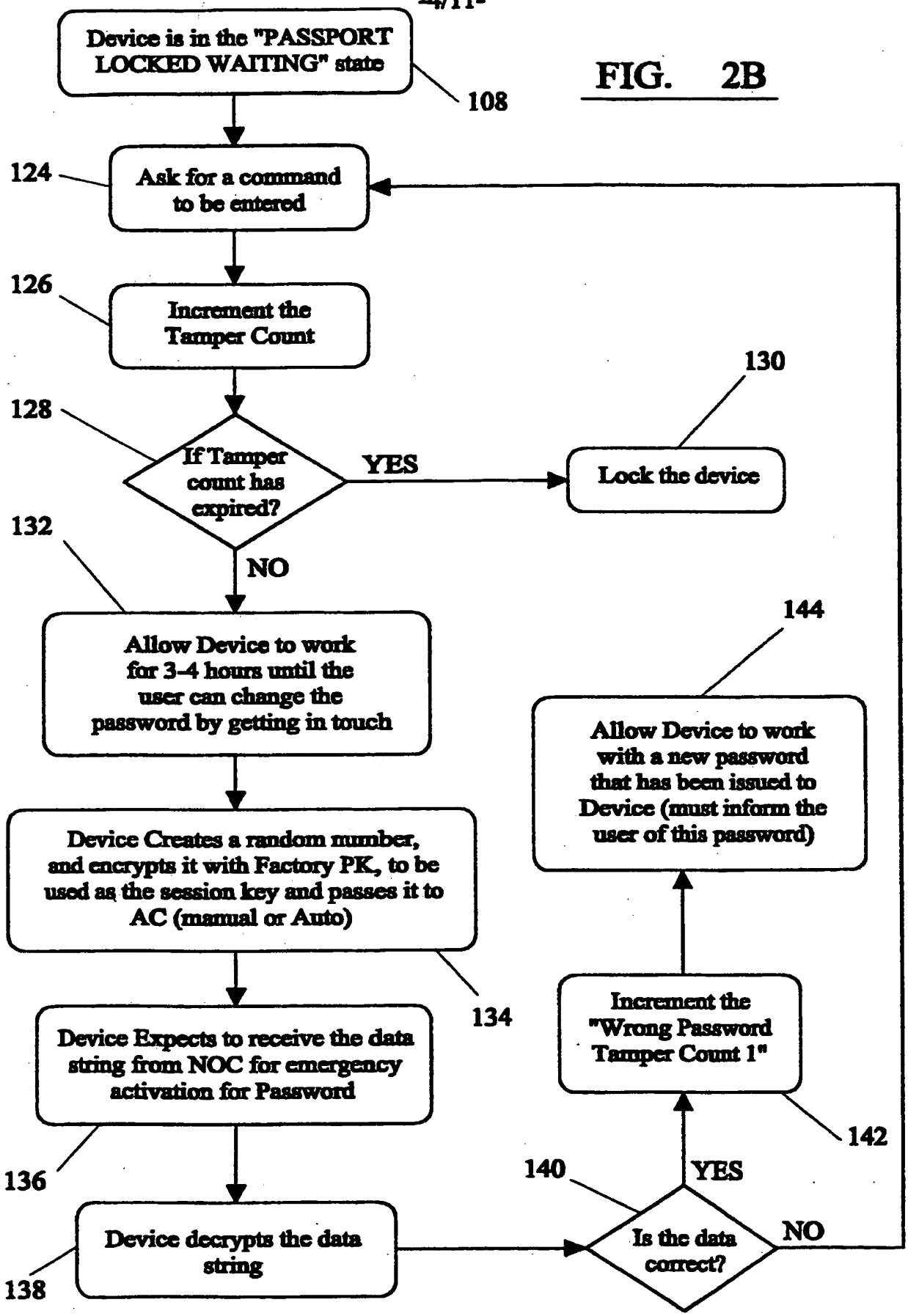
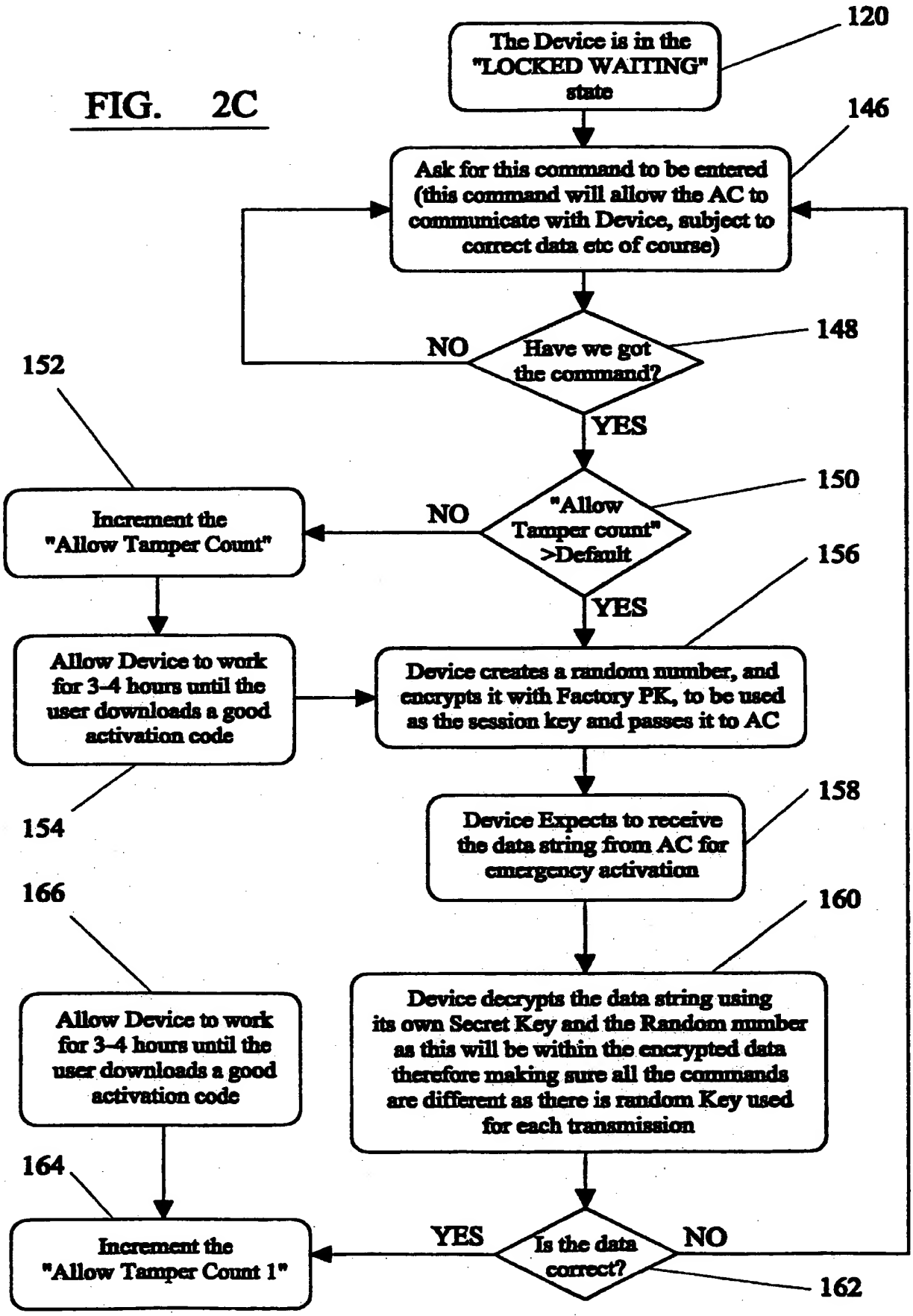

Device is in the "PASSPORT LOCKED WAITING" state
108
124
Ask for a command to be entered
126
Increment the Tamper Count
128
If Tamper count has expired?
YES
130
Lock the device
NO
132
Allow Device to work for 3-4 hours until the user can change the password by getting in touch
Device Creates a random number, and encrypts it with Factory PK, to be used as the session key and passes it to AC (manual or Auto)
134
Device Expects to receive the data string from NOC for emergency activation for Password
136
Device decrypts the data string
138
Is the data correct?
140
YES
NO
Increment the "Wrong Password Tamper Count 1"
142
144
Allow Device to work with a new password that has been issued to Device (must inform the user of this password)

FIG. 2C


120
The Device is in the "LOCKED WAITING" state
146
Ask for this command to be entered (this command will allow the AC to communicate with Device, subject to correct data etc of course)
148
Have we got the command?
NO
YES
150
"Allow Tamper count" >Default
NO
YES
152
Increment the "Allow Tamper Count"
Allow Device to work for 3-4 hours until the user downloads a good activation code
154
156
Device creates a random number, and encrypts it with Factory PK, to be used as the session key and passes it to AC
158
Device Expects to receive the data string from AC for emergency activation
160
Device decrypts the data string using its own Secret Key and the Random number as this will be within the encrypted data therefore making sure all the commands are different as there is random Key used for each transmission
162
Is the data correct?
YES
NO
164
Increment the "Allow Tamper Count 1"
166
Allow Device to work for 3-4 hours until the user downloads a good activation code

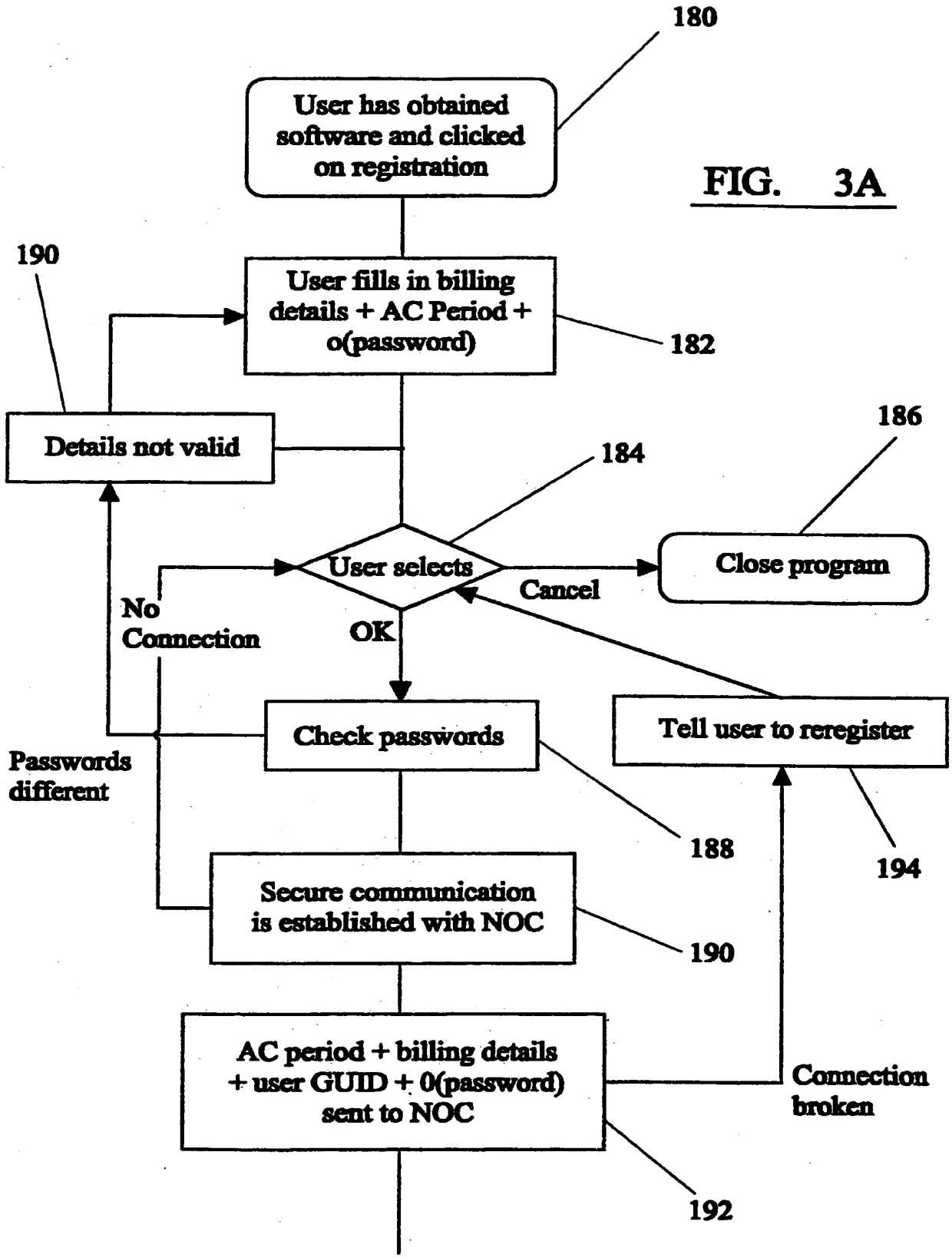

180
User has obtained software and clicked on registration
190
User fills in billing details + AC Period + o(password)
182
Details not valid
184
186
User selects
Close program
Cancel
No Connection
OK
Check passwords
Tell user to reregister
Passwords different
188
194
Secure communication is established with NOC
190
AC period + billing details + user GUID + 0(password) sent to NOC
Connection broken
192

FIG. 3A

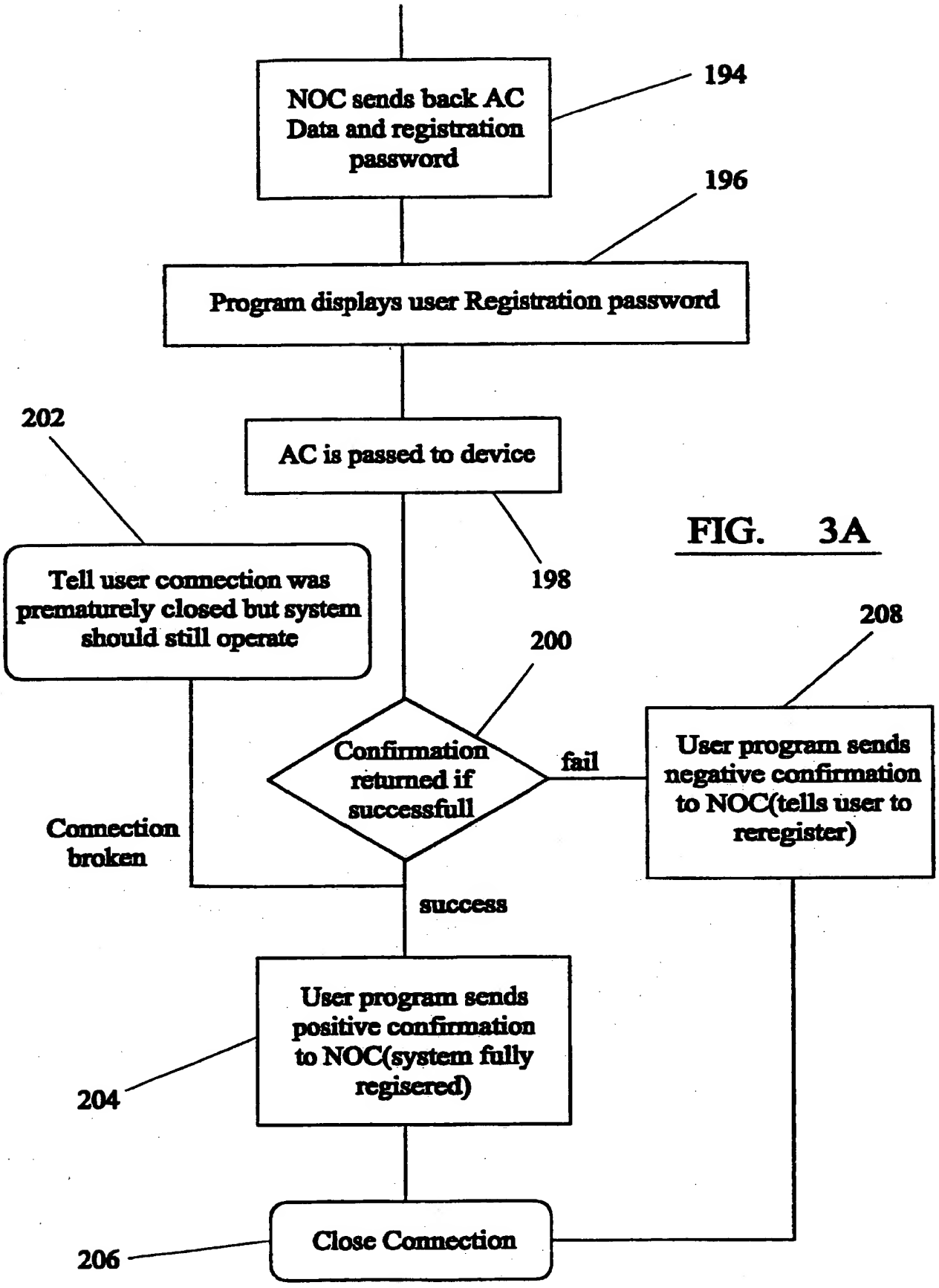

NOC sends back AC Data and registration password
194
196
Program displays user Registration password
202
AC is passed to device
198
Tell user connection was prematurely closed but system should still operate
200
208
Confirmation returned if successfull
fail
User program sends negative confirmation to NOC(tells user to reregister)
Connection broken
success
User program sends positive confirmation to NOC(system fully regisered)
204
Close Connection
206

FIG. 3A

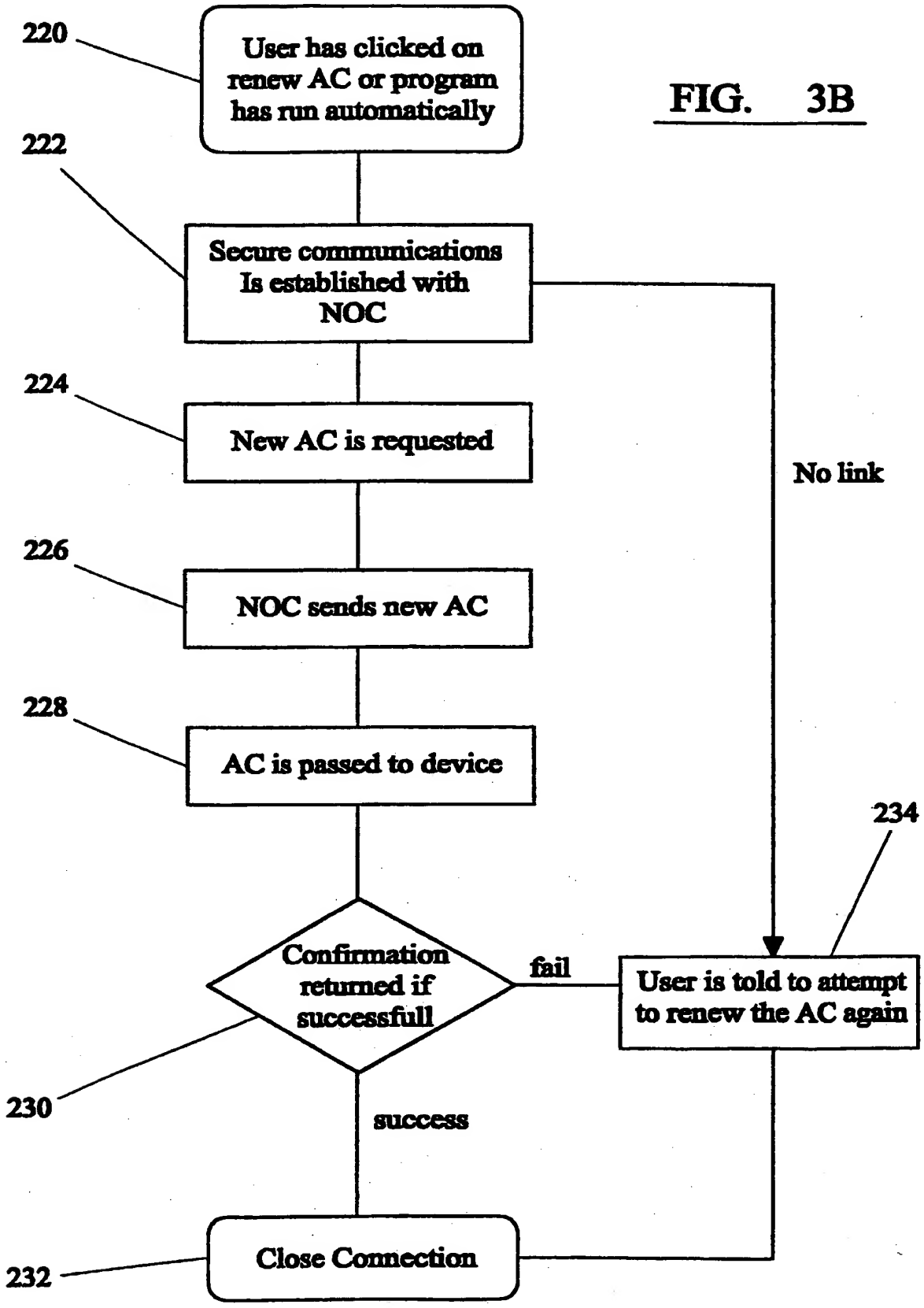

220
User has clicked on renew AC or program has run automatically
222
Secure communications Is established with NOC
224
New AC is requested
226
NOC sends new AC
228
AC is passed to device
Confirmation returned if successfull
fail
No link
234
User is told to attempt to renew the AC again
230
success
Close Connection
232

FIG. 3B

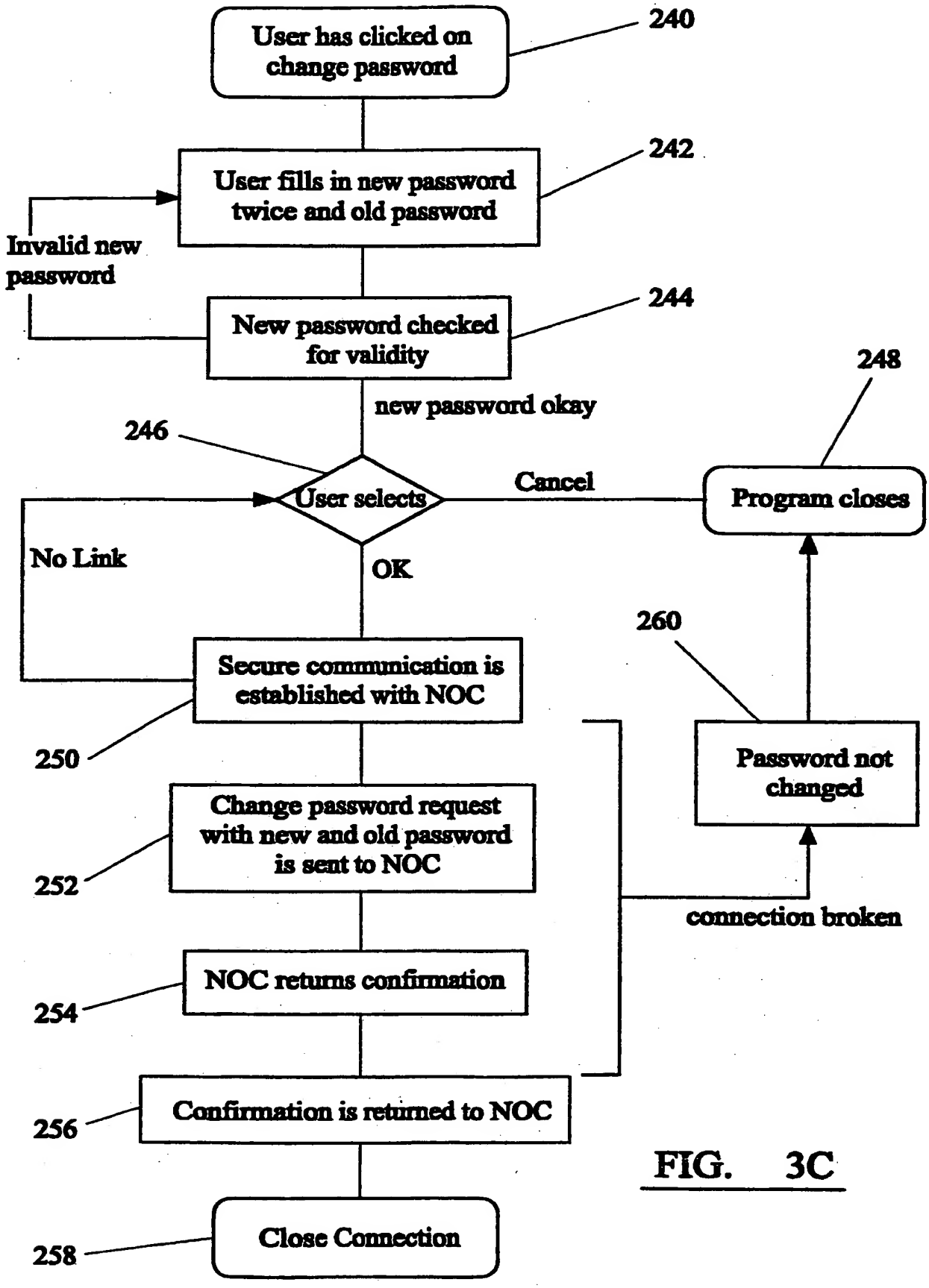
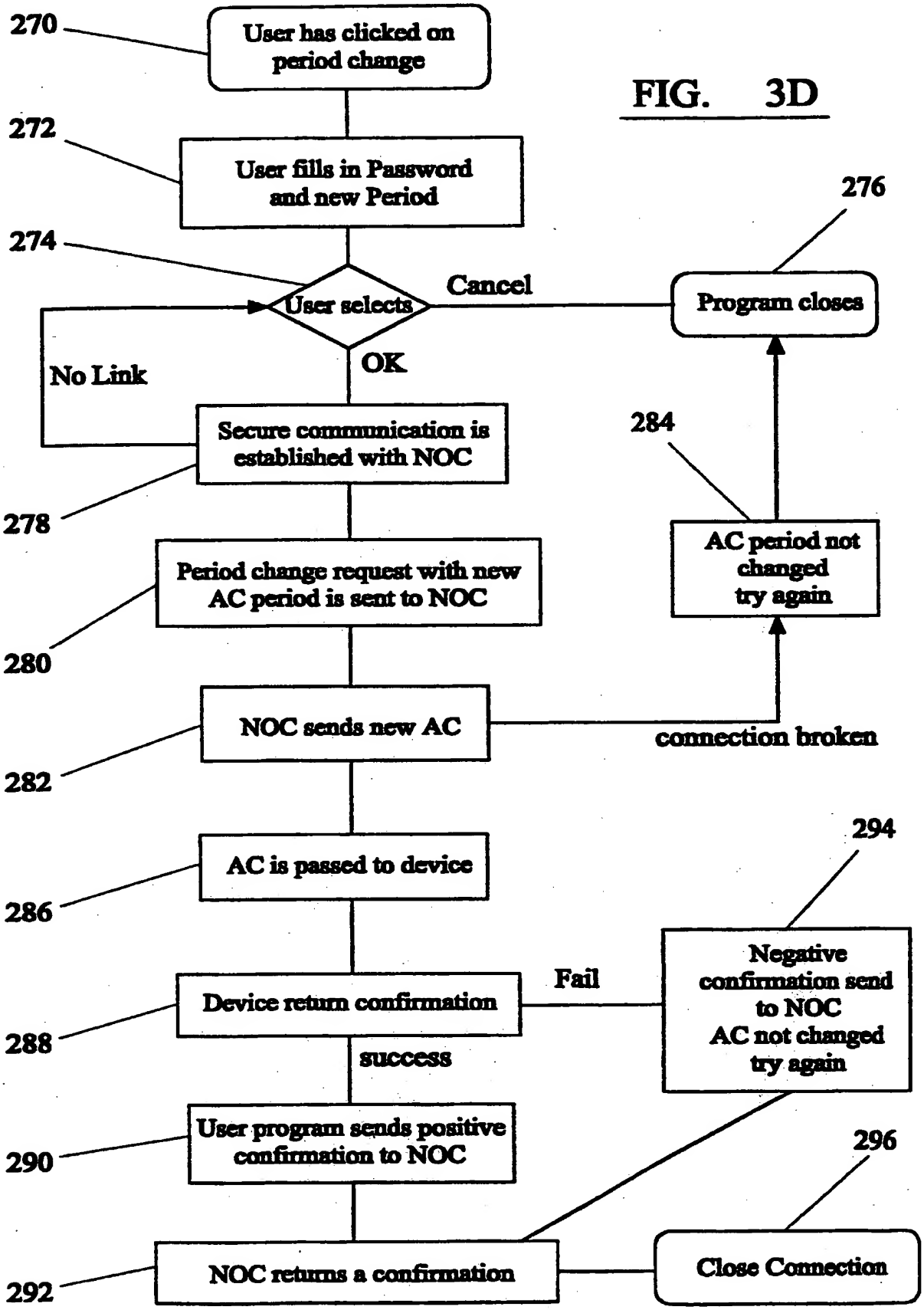

User has clicked on change password
240
User fills in new password twice and old password
242
Invalid new password
New password checked for validity
244
new password okay
246
User selects
Cancel
248
Program closes
No Link
OK
Secure communication is established with NOC
250
260
Password not changed
Change password request with new and old password is sent to NOC
252
connection broken
NOC returns confirmation
254
Confirmation is returned to NOC
256
Close Connection
258

FIG. 3C

FIG. 3D


270
User has clicked on period change
272
User fills in Password and new Period
274
User selects
Cancel
276
Program closes
No Link
OK
Secure communication is established with NOC
278
284
AC period not changed try again
Period change request with new AC period is sent to NOC
280
NOC sends new AC
connection broken
282
AC is passed to device
286
294
Negative confirmation send to NOC AC not changed try again
Fail
Device return confirmation
288
success
User program sends positive confirmation to NOC
290
296
NOC returns a confirmation
Close Connection
292

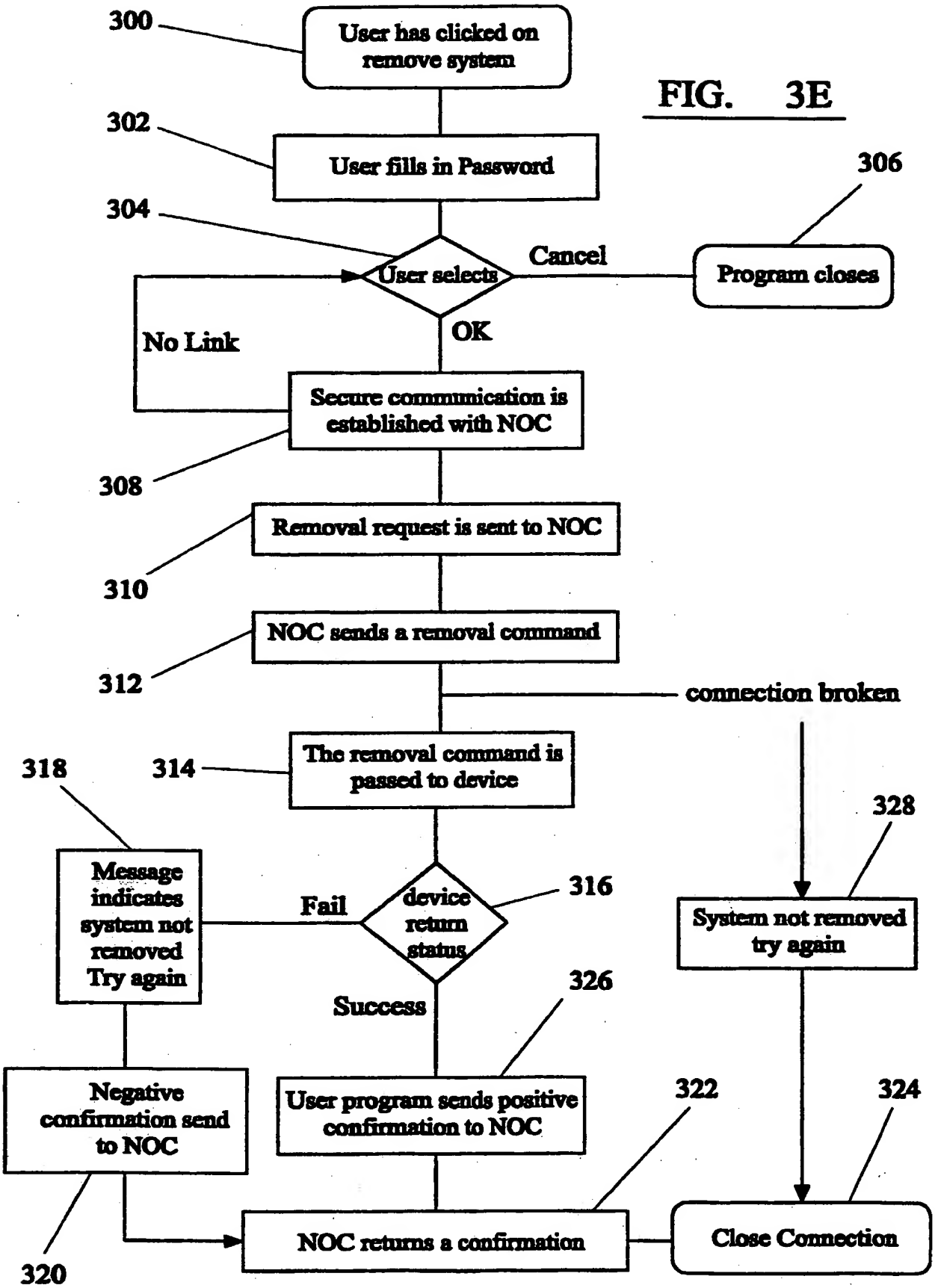

300
User has clicked on remove system
302
User fills in Password
304
User selects
Cancel
306
Program closes
No Link
OK
Secure communication is established with NOC
308
Removal request is sent to NOC
310
NOC sends a removal command
312
connection broken
The removal command is passed to device
314
318
328
Message indicates system not removed Try again
Fail
device return status
316
System not removed try again
Success
326
Negative confirmation send to NOC
User program sends positive confirmation to NOC
322
324
NOC returns a confirmation
Close Connection
320

FIG. 3E